In the claims:

For the Examiner's convenience, all pending claims are presented below with changes shown.

1. (Currently Amended) A method of protecting data within a portable electronic device~~, the method~~ comprising ~~the step of~~:

a user accessing a graphical user interface (GUI) operating on the device to select a predetermined number of attempts for a valid password entry;

determining whether a received password is valid upon detecting an attempt to unlock the device;

determining whether a number of attempts to enter the password exceeds the selected predetermined number of attempts for a valid password entry; and

erasing all applications and data stored on the device if the number of attempts exceed the predetermined number of attempts for a valid password entry.

~~erasing the data after a predetermined number of non-valid passwords are entered that fail to match a valid password.~~

2. (Original) The method according to claim 1 further comprising the steps of: requiring entry of a password to access the data within the portable electronic vice; determining whether the entered password is the valid password; and allowing access to the data if the valid password is entered.

3. (Original) The method according to claim 2 further comprising protecting the data within

the portable electronic device.

4. (Original) The method according to claim 3 where in the step of protecting further comprises encrypting selected data.

5. (Original) The method according to claim 4 further comprising decrypting only a portion of the encrypted selected data being accessed after entry of a valid password.

6. (Original) The method according to claim 1 wherein the step of erasing comprises bit-wiping at least some of the data.

7. (Original) The method according to claim 6 wherein bit-wiping the data comprises overwriting the data with characters.

8. (Original) The method according to claim 7 wherein overwriting the data is performed a plurality of times.

9. (Original) The method according to claim 1 wherein the predetermined number is user defined.

10. (Original) The method according to claim 1 further comprising erasing the data after a predetermined time period from the last syncing of the portable electronic device with another electronic device.

11. (Original) The method according to claim 10 wherein the predetermined time period is user defined.

12. (Original) The method according to claim 2 further comprising locking the portable electronic device and requiring entry of the valid password after a predetermined period of non-operation of a powered on portable electronic device.

13. (Original) The method according to claim 12 wherein the step of locking is performed only after an additional user defined time period after the period of non-operation.

14. (Original) The method according to claim 2 further comprising locking the portable electronic device and requiring entry of the valid password after powering off the portable electronic device.

15. (Original) The method according to claim 2 further comprising disabling data transfer means of the portable electronic device until the valid password is entered.

16. (Original) The method according to claim 2 further comprising protecting the valid password.

17. (Original) The method according to claim 16 wherein protecting the valid password is provided using an MD5 hash.

18. (Original) The method according to claim 2 wherein the step of requiring entry of a password is performed to restrict access to selected applications within the portable electronic device.

19. (Original) The method according to claim 2 further comprising displaying a lockout screen having the appearance of a normal start-up screen of the portable electronic device and having a password entry portion.

20. (Original) The method according to claim 1 wherein the portable electronic device is a personal digital assistant.

21. (Currently Amended) A method of protecting data within a portable electronic device to prevent access the data when in a locked mode, ~~the method~~ comprising ~~the steps of~~:

a user accessing a graphical user interface (GUI) operating on the device to encrypt selected data whenever the device is operating in a locked mode;

the user accessing the GUI to select a predetermined number of attempts for a valid password entry;

determining whether a received password is valid upon detecting an attempt to exit the locked mode;

determining whether a number of attempts to enter the password exceeds the selected predetermined number of attempts for a valid password entry; and

erasing all applications and data stored on the device if the number of attempts exceed the predetermined number of attempts for a valid password entry.

~~encrypting selected data when in the locked mode; and erasing all data after a predetermined number of non-valid passwords are entered that fail to match a valid password.~~

22. (Original) The method according to claim 21 further comprising disabling data transfer means of the portable electronic device in the locked mode.

23. (Original) The method according to claim 21 further comprising requiring entry of the valid password upon powering on the portable electronic device after a previous powering off.

24. (Original) The method according to claim 21 wherein after an automatic powering off of the portable electronic device based upon non-use, the portable electronic device is not locked until a predetermined time period has expired.

25. (Original) The method according to claim 23 further comprising decrypting only a portion of the encrypted selected data accessed after entry of a valid password.

26. (Currently Amended) A portable electronic device comprising:

a graphical user interface (GUI) to select a predetermined number of attempts for a valid password entry;

a data storage component for storing data; and

a processor programmed to erase all applications and data stored ~~data~~ on the data storage component after a predetermined number of non-valid passwords are entered that fail to match a valid password.

27. (Original) The portable electronic device according to claim 26 wherein the processor is further programmed to encrypt selected stored data.

28. (Original) The portable electronic device according to claim 27 wherein the processor is further programmed to decrypt only a portion of the selected stored data being access after entry of the valid password.

29. (Original) The portable electronic device according to claim 26 further comprising a display and wherein the processor is programmed to provide a password entry portion on the display for entering a password.

30. (Original) The portable electronic device according to claim 26 further comprising data transfer means and wherein the processor is programmed to disable the data transfer means until the valid password is entered.

31. (Original) The portable electronic device according to claim 26 further comprising a plurality of buttons for accessing the stored data and wherein the plurality of buttons are adapted to provide for entry of a password.

32. (Original) The portable electronic device according to claim 26 wherein the data storage component comprises a RAM portion and a ROM portion and the processor is programmed to erase all stored data in the RAM after a predetermined number of non-valid passwords are entered that fail to match a valid password.

33. (Currently Amended) A method of protecting data within a portable electronic device~~, the method~~ comprising ~~the step of~~:

determining whether a predetermined time period has expired since the device has been synchronized with a second device; and

erasing all applications and data stored on the device if the predetermined time period has expired.

~~erasing the data after a predetermined time period from the last syncing of the portable electronic device with another electronic device.~~